# LA GEOLOCALIZACIÓN COMO MEDIO DE CONTROL DEL TRABAJADOR

DJAMIL TONY KAHALE CARRILLO

*Profesor Titular de Derecho del Trabajo y de la Seguridad Social*

Universidad Politécnica de Cartagena (UPCT)

**EXTRACTO** **Palabras clave:** Geolocalización; control; GPS; datos; intimidad; control

El empleador puede adoptar todas las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad. En este sentido, aquel puede implementar la geolocalización como medio de control del trabajador.

El presente estudio tiene por objeto analizar la geolocalización como medio de control del trabajador, a través de los dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Por un parte, se estudia los aspectos más importantes para tener en cuenta sobre la geolocalización. Por otra, se analiza la doctrina más relevante del Grupo de Trabajo del artículo 29, que actualmente asume sus funciones el Consejo Europeo de Protección de Datos; seguidamente, se aborda el derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral, con el objeto de estudiar los criterios jurisprudenciales más relevantes. Por último, se presentan las conclusiones más relevantes.

**ABSTRACT** **Key words:** Geolocation, control, GPS, data, privacy, control

The employer may adopt all the measures it deems most appropriate for surveillance and control to verify the worker's compliance with his or her work obligations and duties, with due consideration for his or her dignity in their adoption and application. In this sense, the latter can implement geolocation as a means of worker control.

The purpose of this study is to analyse geolocation as a means of worker control, through the provisions of Organic Law 3/2018, of 5 December, on Personal Data Protection and the guarantee of digital rights. On the one hand, it studies the most important aspects to bear in mind regarding geolocation. On the other, it analyses the most relevant doctrine of the Article 29 Working Group, which is currently assumed by the European Data Protection Board; then, it addresses the right to privacy in the use of geolocation systems in the workplace, with the aim of studying the most relevant jurisprudential criteria. Finally, the most relevant conclusions are presented.

 Recepción original: 03.03.2021. Aceptación: 01.04.2021

**ÍNDICE**



## 1. INTRODUCCIÓN

La transformación digital afecta a la manera en la que los trabajadores prestan sus servicios y a los medios de control que, cada día son más sofisticados y preciso, por parte del empresario con el objeto de supervisar el correcto desempleo de las actividades que realizan aquellos. Las nuevas tecnologías, por tanto, generan una relación contractual no muy protegida que plantea una serie de retos al Derecho del Trabajo como el almacenamiento y tratamiento de datos de información personal, la intimidad del trabajador o el control de los trabajadores mediante programas o herramientas informáticas.

Bajo este contexto, el Derecho del Trabajo debe «esforzarse en asegurar "el equilibrio en el que han de convivir el legítimo interés de la empresa (y del empresario) y el de los propios trabajadores", de modo que "ni el empresario pued[a] ignorar e invalidar la esfera jurídica del trabajo ni éste obstruir el ámbito de poder que compete al patrono"»[1].

El aumento de la cantidad de datos generados en el lugar de trabajo, en combinación con las nuevas técnicas de análisis de datos y la comparación cruzada, entre otras cosas, puede crear el riesgo de un tratamiento posterior incompatible. Por ejemplo, en este sentido, se incluyen el uso de sistemas instalados legítimamente para proteger las propiedades para controlar después la

[1] Esta obra queda enmarcada dentro de los trabajos de investigación desarrollados por el autor en el Proyecto financiado por la Comunidad Autónoma de la Región de Murcia a través de la convocatoria de Ayudas a proyectos para el desarrollo de investigación científica y técnica por grupos competitivos, incluida en el Programa Regional de Fomento de la Investigación Científica y Técnica (Plan de Actuación 2019) de la Fundación Séneca-Agencia de Ciencia y Tecnología de la Región de Murcia: 20976/PI/18: El impacto de la Industria 4.0 en el trabajo: Una visión interdisciplinar; así como en el proyecto: Bargaining upfront in the digital age (VS/2019/0280), financiado por la Comisión Europea.

Montoya Melgar, A., "Poder de dirección y videovigilancia laboral", en AA.VV. (Coords. Monreal Bringsvaerd. E., Thibault Aranda, X. y Jurado Segovia, Á.), *Derecho del Trabajo y Nuevas Tecnologías*, Tirant lo Blanch, Valencia, 2020, págs. 189-190.

disponibilidad, el desempeño y el trato de los trabajadores con los clientes. Otros incluyen el uso de los datos recopilados mediante un sistema de circuito cerrado de televisión para controlar regularmente el comportamiento y el rendimiento de los trabajadores, o el uso de datos de un sistema de geolocalización (seguimiento mediante WiFi o Bluetooth) para comprobar constantemente los movimientos y el comportamiento de un trabajador[2].

El uso de los sistemas de geolocalización trae como consecuencia «intereses empresariales legítimos para velar por el correcto desarrollo del proceso productivo, también existen riesgos respecto del uso que se pueda hacer de los datos potencialmente sensibles obtenidos de la información de la ubicación del trabajador, fundamentalmente cuando además los dispositivos le acompañan fuera de su jornada laboral»[3].

Como resultado, este seguimiento puede infringir los derechos de privacidad de los trabajadores, independientemente de que el control se lleve a cabo de manera sistemática u ocasional. El uso amplio de tecnologías de control, a su vez, puede limitar la disposición de los trabajadores a informar a los empresarios (y los canales por los cuales podrían hacerlo) sobre irregularidades o acciones ilegales de superiores y otros trabajadores que puedan suponer un daño para la empresa (especialmente los datos de los clientes) o el lugar de trabajo.

La privacidad, según la Real Academia Española, en una de sus acepciones, es el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión. Empero, se han dado voces al manifestar que aquella «constituye un conjunto más amplio, más global, de facetas [de la personalidad de un individuo] que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que este tiene derecho a mantener reservado»[4].

La protección de datos, como más adelante se analizará, es muy importante; dado que la legislación la ampara. En este sentido, las causas de la necesidad de su protección se deben a las siguientes circunstancias: a) La era digital; es decir, la rápida evolución de la tecnología, b) La globalización, c) La utilización de datos a grane escala, d) La gran capacidad y rapidez de almacenamiento, procesamiento,

[2] Dictamen 2/2017 sobre el tratamiento de datos en el trabajo. GT 29.

[3] López De La Fuente, G., *La revolución tecnológica y su impacto en las relaciones de trabajo y en los derechos de los trabajadores*, Tirant lo Blanch, Valencia, 2020, pág. 73.

[4] Navalpotro, Y., "Antecedentes de la Ley Orgánica 15/1999 (LOPD)", en Almuzara Almaida, C., *Estudio práctico sobre la protección de datos de carácter personal*, Lex Nova, Madrid, 2005, pág. 40.

manipulación y transmisión de datos personales, e) Necesidad de tutela, f) El riesgo de tratamiento ilegítimo de los datos.

Por ello, se han dado voces al afirmar, por una parte, que «*los derechos fundamentales de las personas trabajadoras no se detienen en la pantalla de los dispositivos digitales, sino que les acompañan durante la navegación por las redes y en el uso de las TIC*. Sería ésta la neo-expresión de la inherencia de los derechos fundamentales de los trabajadores/as en el entorno digital, propio de las relaciones laborales del Siglo XXI, que han mutado el paradigma antropológico del *homo industrailis* al *homo digitalis*, y han trasladado su ecosistema de la fábrica a la red»[5].

Por otra, que «no siempre es fácil discernir la relación, ni la línea de separación, entre lo que ese texto legal ha llamado «derechos digitales» y lo que implica más bien protección de datos personales. En verdad, muchos de los derechos digitales reconocidos con carácter general en la Ley orgánica 3/2018 (neutralidad de internet, acceso universal a internet, rectificación en internet o educación digital) carecen de una relación directa con la protección de datos personales y se conectan más bien con otros derechos básicos o fundamentales de las personas, como la igualdad y no discriminación, la libertad de expresión, la intimidad, el honor o la dignidad»[6].

El presente estudio, por tanto, tiene por objeto analizar la geolocalización como medio de control del trabajador, a través de los dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD)[7]. Por un parte, se estudian los aspectos más importantes para tener en cuenta sobre la geolocalización. Por otra, se analiza la doctrina más relevante del grupo de trabajo del artículo 29, que actualmente asume sus funciones el Consejo Europeo de Protección de Datos; seguidamente, se aborda el derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral, con el objeto de estudiar los criterios jurisprudenciales más relevantes. Por último, se presentan las conclusiones más relevantes.

Para llevar a cabo la investigación se ha requerido de un análisis de la legislación relacionada con el tema a abordar, la jurisprudencia más relevante, la utilización de base de datos e internet y la doctrina más distinguida en la materia.

[5] Preciado Domenech, C., "Monitorización: GPS, Wearables y especial referencia a los controles biométricos para el registro horario. Aspectos procesales", en AA.VV. (Dirs. Rodríguez-Piñero Royo, M. y Todolí Signes, A.), *Vigilancia y control en el Derecho del Trabajo Digital*, Thomson Reuters – Aranzadi, Cizur Menor, 2020, pág. 220.

[6] García Murcia, J. y Rodríguez Cardo, I., "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *Nueva Revista Española de Derecho del Trabajo*, núm. 216, 2019, pág. 31.

[7] BOE núm. 294, de 6 de diciembre de 2018.

## 2. LA GEOLOCALIZACIÓN: ASPECTOS PARA TENER EN CUENTA

La Oficina de Seguridad del Internauta[8] indica que la geolocalización «consiste en obtener la ubicación geográfica de un objeto como puede ser un teléfono móvil, un coche o una calle. Para ello se puede utilizar diferentes métodos como por ejemplo comprobar el código postal de una carta, la dirección IP de un equipo o el sistema GPS de nuestro teléfono móvil»[9].

La geolocalización es conocida, a su vez, por las siglas GPS que significan en inglés *Global Positioning System*; es decir, Sistema de Posicionamiento Global. Que, como ya se ha comentado, es un sistema que permite posicionar cualquier persona u objeto sobre la Tierra con una precisión. Aquel ha sido desarrollado por el ejército estadounidense, cuyos resultados se han aplicado a usos civiles y fundamentalmente en la navegación marítima. Bajo este contexto, los datos de localización se calculan por triangulación y se facilitan de manera directa a la persona que dispone de un receptor GPS[10]. Los datos pueden enviarse a un tercero mediante una red de comunicaciones electrónicas (combinación GPS/GSM)[11].

Desde la óptica de las relaciones laborales, la geolocalización se utiliza por parte del empresario para llevar un control de los trabajadores. No solo se puede implementar por la empresa privada, la Administración pública también pueden implementarlo. No obstante, su implementación, como más adelante se analizará, produce ciertas implicaciones para los derechos fundamentales de los trabajadores[12].

El apartado tercero del artículo 20 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de

[8] La Oficina de Seguridad del Internauta es un organismo que depende actualmente del INCIBE y del Ministerio de Asuntos Económicos y Transformación Digital. Su principal función es ofrecer información y servicios de ciberseguridad a sus visitantes, utilizando para ello un lenguaje accesible, alejado de tecnicismos, de manera que cualquier pueda entender sus contenidos, independientemente de la edad, la formación el grado de conocimientos. www.osi.es

[9] OFICINA DE SEGURIDAD DEL INTERNAUTA, "Geolocalización: virtudes y riesgos", publicado el 20/09/2016, https://www.osi.es/es/actualidad/blog/2016/09/20/geolocalizacion-virtudes-y-riesgos#:~:text=La%20geolocalizaci%C3%B3n%20consiste%20en%20obtener,GPS%20de%20nuestro%20tel%C3%A9fono%20m%C3%B3vil.

[10] La técnica GPS utiliza 31 satélites que giran en 6 órbitas diferentes alrededor de la Tierra, cada satélite transmite una señal radioeléctrica muy precisa. Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes. GT 29.

[11] Dictamen 5/2005 sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido. Grupo del artículo 29.

[12] El Tribunal Constitucional ha dispuesto que en ningún derecho fundamental es absoluto «pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para

los Trabajadores (ET)[13], establece la facultad de control que tiene el empresario al señalar que aquel «podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales», siempre que respete la dignidad del trabajador, así como otros derechos que puedan verse afectados por las medidas que este adopte[14].

Aquellas medidas pueden materializarse, entre otras formas, a través de las nuevas tecnologías. Al facilitarle al empleador un informe de manera detallada, en

alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho». STC 186/2000. En el mismo sentido, las SSTC 57/1994 y 143/1994. Asimismo, los derechos fundamentales «son derechos subjetivos, derechos de los individuos en cuanto garantizan un status jurídico o la libertad de un ámbito de existencia. Pero, al propio tiempo, son elementos esenciales de un ordenamiento objetivo de la comunidad nacional, en cuanto ésta se configura como un marco de una convivencia humana justa y pacífica, plasmada históricamente en el Estado de derecho y, más tarde, en el Estado social de derecho o el Estado social y democrático de derecho, según la fórmula de nuestra Constitución (art. 1.1)». STC 25/1981.

[13] BOE núm. 255, de 24 de octubre de 2015.

[14] Si bien el tratamiento de los datos de carácter personal requiere la información y el consentimiento inequívoco del afectado, en el ámbito laboral el consentimiento del trabajador pasa, como regla general, a un segundo plano pues el consentimiento se entiende implícito en la relación negocial, siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento del contrato firmado por las partes. Sin embargo, el consentimiento de los trabajadores afectados sí será necesario cuando el tratamiento de datos se utilice con finalidad ajena al cumplimiento del contrato. Ahora bien, aunque no sea necesario el consentimiento, el deber de información sigue existiendo. En el caso concurre una falta de acreditación de que se hubiera informado expresamente al trabajador de la existencia del sistema de grabación, ni que éste tuviera conocimiento de ello, ni que la empresa hubiera colocado los distintivos genéricos de la Agencia de Protección de Datos. En aplicación de la doctrina emanada del TEDH, es transcendente si se obvia la información previa de la existencia de sospechas razonables de que se había cometido una infracción grave, al no verse comprometida la propiedad con pérdidas de alcance y sin que se genere una situación en la que el buen funcionamiento de una empresa esté en riesgo, al no existir sospecha de una acción concertada por parte de varios empleados, creando así una atmósfera general de desconfianza en el lugar de trabajo. STSJ de Madrid, de 16 de enero de 2020. La empresa informó a los trabajadores de que se instalaba un sistema de videovigilancia mediante cámaras en el interior del local de la empresa para garantizar la seguridad de los trabajadores, clientes y usuarios. Se indicaba que la información obtenida se utilizaría para fines de prevención, seguridad y protección y para el control de calidad, así como para la verificación del cumplimiento por el trabajador de sus obligaciones y deberes laborales. Asimismo, se informaba que se garantizaba la confidencialidad y seguridad de las imágenes, que se utilizarían exclusivamente para las finalidades perseguidas, y que serían borradas en los períodos establecidos legalmente. Se informaba a los trabajadores de los derechos de acceso, rectificación, limitación del tratamiento, supresión y portabilidad mediante las oportunas solicitudes por escrito. La representación legal de los trabajadores remitió comunicación a la empresa indicando que esta medida no había sido consensuada ni negociada con la representación de los trabajadores y que no se había informado con carácter previo y pedía información adicional. La empresa contestó comunicando los datos relativos al número y localización de cada cámara, capacidad de las cámaras, con indicación de que no se instalaba grabación de audio, instalaciones

este caso, de los sitios que su plantilla visite durante la jornada laboral. El peligro de ello radica en que debe mantenerse un equilibrio entre la facultad de control del empresario y los derechos de los trabajadores. Por lo que «se introduce un elemento nuevo en el sinalagma contractual capaz de provocar la ruptura en el necesario equilibrio de intereses» entre las partes[15].

Dicho de otra manera, la utilización de la geolocalización en las relaciones laborales tiene implicaciones, por una parte, para el derecho fundamental a la intimidad. Por otra, a la protección de datos personales. En cuanto a este último punto, el trabajador queda sujeto a la LOPD, puesto que será aplicable a cualquier tratamiento total o parcialmente automatizado de datos personales, según dispone el primer apartado del artículo 2. Por consiguiente, los empleadores que utilicen la geolocalización tendrán que cumplir con lo establecido en aquella norma cuando corresponda a datos personales de la plantilla.

Antes de seguir avanzando hay que matizar que «la promulgación de una norma específica en materia de protección de datos aplicable a los centros de trabajo, aunque supone un avance, no resuelve (…) todos los problemas suscitados en el ámbito laboral, dadas las situaciones heterogéneas y cambiantes en los diversos sectores productivos y, sobre todo, la constante innovación tecnológica y sus efectos en el seno de la empresa»[16].

Retomando el tema de estudio, el uso de aquellos dispositivos que tengan dicha tecnología dará lugar a un tratamiento de datos personales. Huelga recordar que el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (RGPD)[17], define datos personales como «toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o

objeto de grabación, las necesidades motivadoras de la medida, destino y lugar de almacenamiento de la información obtenida. Entiende la Sala que, por parte de la empresa, se ha cumplido con la obligación de información previa a los trabajadores sobre los sistemas de videovigilancia, número de cámaras y espacios de la empresa objeto de vigilancia. Asimismo, se ha justificado por la empresa dicha instalación en los fines de seguridad de personas y cosas y verificación del cumplimiento por el trabajador de sus obligaciones y deberes laborales. Además, se indica que no está operativo el sistema de grabación de audio y que las máquinas están en las zonas de almacén y producción, no en áreas de descanso, aseos o vestuarios. STSJ del País Vasco, de 12 de noviembre de 2019.

[15] Fernández Domínguez, J. y Rodríguez Escanciano, S., *Utilización y control de datos laborales automatizados*, Agencia de Protección de Datos, Madrid, 1997, pág. 87.

[16] Rodríguez Escanciano, S., *Derechos laborales digitales: Garantías e interrogantes*, Thomson Reuters – Aranzadi, Cizur Menor, 2019, pág. 31.

[17] DOUE núm. 119, de 4 de mayo de 2016.

indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona». Por tanto, entraría en juego los datos de localización.

La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)[18], define datos de localización como «cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público».

Bajo este contexto, aquella norma dispone que, en el supuesto de que puedan tratarse datos de localización, diferentes de los datos de tráfico, relativos a los usuarios o abonados de redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público, solo podrán tratarse dichos datos si se hacen anónimos. Salvo que previo consentimiento de los usuarios o abonados, en la medida y por el tiempo necesario para la prestación de un servicio con valor añadido. Empero, el proveedor del servicio deberá informar a los usuarios o abonados, antes de obtener su consentimiento, del tipo de datos de localización distintos de los datos de tráfico que serán tratados, de la finalidad y duración del tratamiento y de si los datos se transmitirán a un tercero a efectos de la prestación del servicio con valor añadido. Por lo que se deberá ofrecer a los usuarios y abonados la posibilidad de retirar en todo momento su consentimiento para el tratamiento de los datos de localización diferentes de los datos de tráfico.

En el supuesto de que se haya obtenido el consentimiento de un usuario o abonado para el tratamiento de datos de localización diferentes de los datos de tráfico, el usuario o abonado deberá seguir contando con la posibilidad, por un procedimiento sencillo y gratuito, de rechazar de manera temporal el tratamiento de aquellos datos para cada conexión a la red o para cada transmisión de una comunicación. Podrán encargarse del tratamiento de datos de localización diferentes de los datos de tráfico solo aquellas personas que actúen bajo la autoridad del proveedor de las redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público o del tercero que preste el servicio con valor añadido, y dicho tratamiento deberá limitarse a lo necesario a efectos de la prestación del servicio con valor añadido.

La definición antes mencionada es similar a la que señala el legislador español en el artículo 64 b) del Real Decreto 424/2005, de 15 de abril, por el que

[18] DOCE núm. 201, de 31 de julio de 2002.

se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios[19].

Aquella norma está sujeta a la LOPD, dado que los datos de localización se refieren a una persona física identificable, que constituyen datos personales. Empero, no define la geolocalización; pero si hace su mención en el siguiente articulado, que más adelante se analizará:

a) Artículo 90: Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral

b) Disposición final decimotercera: Modificación del texto refundido de la Ley del Estatuto de los Trabajadores.

c) Disposición final decimocuarta. Modificación del texto refundido de la Ley del Estatuto Básico del Empleado Público.

## 3. EL GRUPO DE TRABAJO DEL ARTÍCULO 29 (GT 29): ACTUAL CONSEJO EUROPEO DE PROTECCIÓN DE DATOS

Hay que resaltar que, a partir del 25 de mayo de 2018, el Grupo de Trabajo del artículo 29 dejó de existir y fue sustituido por el Consejo Europeo de Protección de Datos (EDPB)[20]. No obstante, hay que hacer mención del origen de dicho grupo para poder comprender su labor en el tema de estudio. El Grupo de Trabajo del Artículo 29 (GT 29), creado por la Directiva 95/46/CE (RGPD), era un órgano consultivo independiente integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea – que realizaba funciones de secretariado-. Las autoridades de los Estados candidatos a ser miembros de la Unión Europea (UE) y los países del EEE asistían a sus reuniones como observadores. En este sentido, la Agencia Española de Protección de Datos[21] formó parte de aquel desde su inicio, en febrero de 1997.

El GT 29 contaba con un presidente y dos vicepresidentes, elegidos de entre sus miembros por periodos de dos años, renovables. Se reunían en plenarios con

[19] BOE núm. 102, de 29 de abril de 2005.

[20] El sitio web de la EDPB se puede consultar en la siguiente dirección: https://edpb.europa.eu/

[21] La Agencia Española de Protección de Datos es la autoridad pública independiente encargada de velar por la privacidad y la protección de datos de los ciudadanos. https://www.aepd.es/es

una periodicidad bimestral y organizaba sus trabajos mediante distintos subgrupos temáticos, que preparaban las decisiones del plenario.

Las funciones del GT29 reconocidas por la Directiva incluían estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la Directiva, emitir dictámenes sobre el nivel de protección existente dentro de la Comunidad y en países terceros, asesorar a la Comisión sobre cualquier proyecto de modificación de la Directiva, y formular recomendaciones sobre cualquier asunto relacionado con la protección de datos en la UE.

Aquel ente se pronunciaba mediante Dictámenes, Documentos de Trabajo, Informes o Recomendaciones, aunque también manifestaba su posición en cartas o comunicados de prensa. Las decisiones del Grupo no eran jurídicamente vinculantes, pero tenían un importante valor doctrinal y son frecuentemente utilizados y citados por los legisladores y los tribunales nacionales y europeos[22]. Por ello de su importancia para este estudio.

Bajo este contexto, se pasará a analizar los criterios del GT29 en relación con la geolocalización, por el valor doctrinal que tienen. Las aplicaciones o plataformas que requieren acceso a la geolocalización deben usar los servicios de localización del sistema operativo. «Cuando una aplicación use la geolocalización, el sistema operativo puede recoger datos personales para transmitir datos de geolocalización a las aplicaciones y también puede considerar el uso de los datos para mejorar sus propios servicios de localización. A tal efecto, se considera que el sistema operativo es el responsable del tratamiento»[23].

El tratamiento de estos datos es un asunto especialmente sensible «por referirse a la cuestión esencial de la libre circulación de las personas de forma anónima, el legislador europeo, teniendo en cuenta las consideraciones de las autoridades europeas de protección de datos, ha adoptado normas específicas que establecen la obligación de recabar el consentimiento de los usuarios o abonados antes de proceder al tratamiento de los datos de localización necesarios para prestar un servicio con valor añadido y de informar a los usuarios o abonados de las condiciones de dicho tratamiento (Artículo 9 de la Directiva 2002/58/CE de 12 de julio de 2002)»[24].

En vista de la intromisión que la geolocalización supone en el derecho fundamental a la protección de datos, el consentimiento resulta igualmente exigible, con carácter general, al amparo del RGPD, siempre que el tratamiento vaya dirigido a la identificación, directa o indirecta, de la persona. «Dada la sensibilidad del procesamiento de los datos o pautas de datos de localización, el consentimiento

[22] https://ec.europa.eu/newsroom/article29/news-overview.cfm

[23] Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes. GT 29.

[24] Dictamen 5/2005 sobre el uso de los datos de geolocalización. GT 29.

fundamentado previo constituye también el principal factor aplicable para dar legitimidad al tratamiento de datos en lo que se refiere al procesamiento de las localizaciones de un dispositivo móvil inteligente en el contexto de servicios de la sociedad de la información»[25].

En cuanto a los dispositivos de seguimiento de vehículos no son dispositivos para la localización de trabajadores, «ya que su función es hacer un seguimiento o vigilar la ubicación de los vehículos en que estén instalados. Los empresarios no deben considerarlos como dispositivos para seguir o el comportamiento o el paradero de los conductores o de otro tipo de personal, por ejemplo, mediante el envío de alertas relacionadas con la velocidad del vehículo»[26].

No obstante, el tratamiento de los datos de localización puede estar justificado «si se lleva a cabo formando parte del control del transporte de personas o bienes o de la mejora de la distribución de los recursos para servicios en puntos remotos (por ejemplo, la planificación de operaciones en tiempo real) o cuando se trate de lograr un objetivo de seguridad en relación con el propio empleado o con los bienes o vehículos a su cargo. Por el contrario, el Grupo considera que el tratamiento de datos es excesivo en el caso de que los empleados puedan organizar libremente sus planes de viaje o cuando se lleve a cabo con el único fin de controlar el trabajo de un empleado, siempre que pueda hacerse por otros medios»[27].

Ejemplo de consentimiento específico es que una «aplicación ofrece información sobre restaurantes cercanos. Para instalarla, el desarrollador debe obtener el consentimiento. Para acceder a los datos de geolocalización, el desarrollador de aplicaciones debe pedir el consentimiento por separado, por ejemplo, durante la instalación o antes de acceder a la geolocalización.

«Específico» significa que el consentimiento debe limitarse al objetivo concreto de informar al usuario sobre restaurantes próximos. Por tanto, solo puede accederse a los datos de localización del dispositivo cuando el usuario utiliza la aplicación a tal efecto. El consentimiento del usuario para procesar datos de geolocalización no permite a la aplicación la recogida continua de datos de localización del dispositivo. Este tratamiento adicional requeriría información adicional y un consentimiento por separado.

Del mismo modo, para que una aplicación de comunicaciones acceda a la lista de contactos, el usuario debe poder seleccionar los contactos con que desea

[25] Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes. GT 29.

[26] Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes. GT 29.

[27] Dictamen 5/2005 sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido. GT 29.

comunicarse, en lugar de tener que dar acceso a toda la lista de contactos (incluidos los datos de contacto de quienes no son usuarios de ese servicio, que no pueden haber dado su consentimiento al tratamiento de los datos que les afectan)»[28].

Como puede observarse, los documentos del GT 29 son de gran importancia, a pesar de que no son jurídicamente vinculantes, tenían un significativo valor doctrinal y, hoy por hoy, siguen utilizados y citados por los legisladores y los tribunales nacionales y europeos, así como los investigadores, como es en este estudio.

## 4. EL DERECHO A LA INTIMIDAD ANTE LA UTILIZACIÓN DE SISTEMAS DE GEOLOCALIZACIÓN EN EL ÁMBITO LABORAL

En este epígrafe se estudiará lo señalado en la LOPD. No obstante, hay que destacar que el RGPD establece una serie de principios básicos, con relación al tratamiento de los datos personales[29]:

a) Licitud, lealtad y transparencia: Tratar los datos de manera licita, leal y transparente. Se pueden tratar solo si el responsable tiene una base legítima para hacerlo.

b) Limitación de la finalidad: Tratar los datos recogidos solo para fines determinados, explícitos y legítimos.

c) Minimización de datos: Solicitar datos adecuados, pertinentes y limitados a los necesario a los fines para los que son tratados.

d) Limitación del plazo de conservación: Utilizar los datos durante no más tiempo del necesario para los fines del tratamiento por lo que se solicitaron.

e) Integridad y confidencialidad: Aplicar las medidas de seguridad técnicas u organizativas necesarias que garanticen su seguridad y confidencialidad, así como realizar de manera periódica dichas medidas.

f) Responsabilidad proactiva: El responsable del tratamiento será el responsable de garantizar el respecto a los principios mencionados y ser capaza de demostrarlo.

El artículo 90 de la LOPD dispone que los empresarios podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del ET y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

[28] Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes. GT 29.

[29] Art. 5 RGPD.

No obstante, el legislador deja claro que, con carácter previo, los empresarios habrán de informar de manera expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

El apartado tercero del artículo 20 del ET, bajo este contexto, dispone que el empleador podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad.

Como puede observarse, de su literalidad, el legislador no señala de manera expresa cuáles son los límites para el ejercicio del poder de control empresarial, dado que se intuye de que aquellos existen por lo que deben interpretarse bajo la protección constitucional de los trabajadores. Queda claro que el legislador ha querido hacer énfasis en que el empleador debe, al igual que lo que sucede con la videovigilancia[30], informar de manera expresa, clara e inequívoca a la plantilla con relación a la existencia y características de los dispositivos con geolocalización.

Llama la atención que el legislador no haga mención sobre el principio de proporcionalidad que ha sido debatido a nivel judicial. Por lo que se intuye que la finalidad que persigue la norma es positivar el derecho a la intimidad de los trabajadores que el principio de proporcionalidad, «por lo que parece indicar que ahora no sería posible una medida disciplinaria procedente cuando no ha existido esta información previa a los trabajadores de la instalación de estos dispositivos»[31].

El derecho a la intimidad, por tanto, «no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya que experimentar y se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho»[32]. Bajo este contexto, «el contrato de trabajo no puede considerarse como un título legitimador

[30] *Vid*. González Diaz, F., "Control y límites en el uso de dispositivos de videovigilancia en el marco de la relación laboral", en AA.VV. (Dir. Kahale Carrillo, D.), *El impacto de la industria 4.0 en el trabajo: Una visión interdisciplinar*, Thomson Reuters – Aranzadi, Cizur Menor, 2020, págs. 59-89.

[31] Aragüez Valenzuela, L., "Relación laboral digitalizada en término de justicia y control tecnológico: especial referencia al sistema de geolocalización", en (Dirs. Rodriguez-Piñero Royo, M. y Todolí Signes, A.), *Vigilancia y control en el Derecho del Trabajo Digital*, Thomson Reuters – Aranzadi, Cizur Menor, 2020, pág. 212.

[32] SSTC 57/1994, de 28 de febrero y 143/1994, de 9 de mayo.

de recortes en el ejercicio de los derechos fundamentales que incumben al trabajador como ciudadano, que no pierde su condición de tal por insertarse en el ámbito de una organización privada»[33].

Por consiguiente, aquel principio es de importante aplicación cuando se determine la adecuación de la medida de la geolocalización implementada, «de modo que deberá quedar acreditada la existencia de una necesidad específica de la empresa (control del transporte de personas o bienes, objetivos de seguridad, planificación en tiempo real, seguimiento o facturación) para que puedan establecerse este tipo de sistemas»[34].

El ejercicio de funciones de control fundado en el uso de sistemas de geolocalización tiene que ejercerse según el ordenamiento jurídico establecido y con los límites inherentes a aquel. Dicho de otra manera, la legitimidad del uso de la geolocalización en las relaciones laborales viene impuesta por el cumplimiento del marco legal correspondiente en cada supuesto.

La Disposición final decimotercera de la LOPD añade el artículo 20 bis al ET, al disponer que «los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales».

En el mismo sentido, añade una nueva letra j bis) en el artículo 14 del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público[35], al señalar que los empleados públicos tienen el siguiente derecho, ente otros, de carácter individual en correspondencia con la naturaleza jurídica de su relación de servicio a «la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales».

Hay que destacar, que la protección de datos se diferencia con el derecho a la intimidad en su contenido. Este último confiere a la persona el poder de imponer a terceros el derecho de abstenerse de toda intromisión en la esfera de la persona y la prohibición del uso de su contenido. Mientras que el primero, el derecho a protección de datos, permite a toda persona física que la información sobre sí misma identificada o identificable sea objeto de tratamiento para fines concretos

[33] STC 88/1985, de 19 de julio.

[34] Mercader Uguina, J., *El futuro del trabajo en la era de la digitalización y la robótica*, Tirant lo Blanch, Valencia, 2017, pág. 152.

[35] BOE núm. 261, de 31 de octubre de 2015.

y en base a su consentimiento u otro fundamento legítimo establecido de manera legal[36].

## 5. CRITERIOS JURISPRUDENCIALES

En este apartado se pasará a destacar las sentencias más relevantes relacionadas con el objeto de estudio; es decir, a la geolocalización como medio de control del trabajador. Los datos de los trabajadores obtenidos, a través de la geolocalización, y su tratamiento están protegidos por el artículo 18 de la CE[37], dado que «permiten conocer en todo momento durante su uso parcelas de la vida del trabajador que por muy imbricadas que estén en el desarrollo de la relación laboral con la empresa inciden potencialmente en la esfera de su derecho a la intimidad personal y, de ser objeto de tratamiento al que le asiste la protección de datos de tal carácter»[38].

Aquel precepto constitucional «no aporta por sí solo una protección suficiente frente a las realidades nuevas derivadas del progreso tecnológico, y que el constituyente, en el apartado 4 del precepto, pone de manifiesto la existencia de los riesgos asociados a ese progreso, encomendando al legislador el desarrollo de un instituto de garantía como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona»[39].

Hay que recordar que el empresario para ejercer la facultad de control no requiere el consentimiento del trabajador; no obstante, aquel deberá ser informado de los medios de control adoptados por el empleador, así como la finalidad para la que han sido implantados. Asimismo, quién será la persona responsable del fichero de almacenamiento de datos y el tratamiento que ser dará a los mismos[40]; y cómo

[36] Poquet Catalá, R., "Últimos perfiles del sistema de geolocalización como instrumento del empresario", en AA.VV. (Dirs. Rodríguez-Piñero Royo, M. y Todolí Signes, A.), *Vigilancia y control en el Derecho del Trabajo Digital*, Thomson Reuters – Aranzadi, Cizur Menor, 2020, pág. 179.

[37] Art. 18 de la CE:

«1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

[38] STSJ Madrid, de 21 de marzo de 2014 (rec.1952/2013).

[39] STC 58/2018, de 4 de junio.

[40] El Informe 193/2008 Agencia Española de Protección de Datos, en cuanto a la instalación de un sistema GPS en el automóvil facilitado a un trabajador, en el que tras reproducir el mandato del artículo 20.3 del ET señala que «la existencia de esta legitimación no excluye el cumplimiento

el trabajador debe ejercitar sus derechos de acceso, rectificación, cancelación y oposición de estos.

Dicho de otra manera, si uno de los pilares fundamentales para la licitud del control de los desplazamientos por medio de geolocalización es que la existencia de una relación laboral faculta a la empresa para ejercer sus facultades de control, ello conlleva que «cuando finaliza la jornada laboral o acaba el tiempo de trabajo, dichas facultades empresariales desaparecen y a partir de ese momento es imprescindible el consentimiento de los trabajadores para mantener en funcionamiento los dispositivos GPS»[41].

Por lo que es «indiferente que los trabajadores se hagan cargo de los vehículos que utilizan» una vez finalizada la jornada laboral, sin que el poder de control empresarial dirigido a controlar y garantizar la integridad de estos dispositivos sea suficiente para prescindir del necesario consentimiento de los afectados. En este sentido, «la protección por la empresa de sus bienes y el control del uso que de ellos se haga una vez terminada la jornada de trabajo no constituye una excepción a la vigencia de la indicada regla general del consentimiento»[42].

El derecho a la intimidad resulta afectado «si el empresario utiliza un sistema de control del trabajo de sus empleados que se desarrolla fuera de sus dependencias a través de un sistema de localización permanente del teléfono móvil que se facilitan como instrumento de trabajo sin consentimiento ni conocimiento de aquellos, máxime si estos han de tenerlo a su disposición en todo momento por estar sujetos a disponibilidad permanente»[43].

Sin embargo, no se puede considerar vulnerado el derecho a la intimidad del trabajador, en el caso de que «todos los comerciales conocían la instalación de estos dispositivos porque los mismos emitían un sonido cuando se abre el vehículo y se apaga al introducir la llave». Por tanto, «controlar el destino de sus vehículos y el modo de prestación del servicio por unos comerciales que pasaban buena parte de su jornada fuera del centro de trabajo». En el que el «GPS permanecía inactivo durante los días de vacaciones y fines de semana» se considera que dicha medida es la idónea con relación al fin perseguido[44].

del deber de informar, por parte del empresario previsto en el artículo 5.1 de la Ley Orgánica. En consecuencia, la actuación descrita en la consulta, genera el correspondiente fichero y en todo caso, será obligatoria su inscripción en el Registro General de Protección de Datos, conforme a lo establecido en el artículo 26 de la Ley Orgánica».

[41] STSJ Asturias, de 27 de diciembre de 2017 (rec. 2241/2017).

[42] STSJ Asturias, de 27 de diciembre de 2017 (rec. 2241/2017).

[43] STSJ País Vasco, de 2 de julio de 2007 (rec. 1175/2007).

[44] STSJ Comunidad Valenciana, de 2 de mayo de 2017 (rec. 3689/2016),

En este sentido, en cuanto al derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral, el legislador ha señalado, en el artículo 87 de la LOPD, que los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador. Por tanto, el empresario podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores con el propósito de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

Asimismo, deberán establecer criterios de utilización de los dispositivos digitales respetando los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos en el ordenamiento jurídico. El legislador ha querido dejar claro que, en su elaboración, deberán participar los representantes de los trabajadores.

El acceso por el empresario al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores; como, por ejemplo, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados. Empero, los trabajadores deberán ser informados de los criterios de utilización a lo que se ha hecho referencia.

Con relación a las nociones de centro de trabajo y a los nuevos sistemas de control de la actividad laboral, se ha manifestado que el «centro de trabajo potencialmente es ahora todo aquel que pueda ser objeto de geolocalización y el tiempo de trabajo también puede ser potencialmente todo aquel en el que la actividad pueda prestarse empleando las TIC (…) No es preciso el control directo por otra persona, el mando intermedio, ya que esta tarea puede encomendarse a sistemas de control automatizados sean cámaras, ordenadores, sistemas de geolocalización etc. Y además las TIC permiten acceder a un gran volumen de información y a su tratamiento rápido y barato mediante la creación de los correspondientes algoritmos que a través de la elaboración de perfiles acceden al conocimiento detallado de cuándo, cómo, dónde y con qué resultado se ha trabajado»[45].

El Tribunal Constitucional, en cuanto a los derechos fundamentales, ha señalado que aquellos «no implican privar al empresario de utilizar medios que supongan una intromisión en los mismos, puesto que los derechos fundamentales no tienen carácter absoluto, y pueden ser objeto de limitaciones, siempre que estas

[45] SJS núm. 33 de Madrid, de 11 de febrero de 2019. En los mismos términos, SJS núm. 1 de Madrid, de 4 de abril de 2019.

tiendan de forma exclusiva y proporcionada a la protección de otros derechos y valores, como son la propiedad privada el empresario y la libertad de empresa»[46].

En el supuesto de una empresa que ofrece el servicio de que los clientes pueden saber dónde está su pedido a través de la geolocalización (Proyecto Tracker) se ha indicado que «si bien obedece a fines constitucionalmente legítimos en el desarrollo del derecho a la libre empresa como son el control del empleado en el desempeño de su puesto de trabajo y la oferta de un mejor servicio al cliente – de forma que éste pueda conocer en todo momento la ubicación de su pedido, dotando a la empresa de capacidad para proporcionar servicios que se afirma ya ofrecen otras empresas del sector- no supera a juicio de la Sala el necesario juicio de proporcionalidad (…) para la implantación del sistema de geolocalización por parte del empleador se ha prescindido de proporcional a los trabajadores la información a la que se refieren los arts. 12 y 13 LOPD»[47]. De igual manera, se vulnera lo dispuesto en el segundo apartado del artículo 90 de la LOPD.

Dicho en otros términos, la implantación unilateral por la empresa de aquel proyecto, en virtud del cual los repartidores son geolocalizados cuando realicen tareas de reparto mediante una app descargada en su teléfono móvil personal –que deben aportar a la actividad empresarial–, de manera que los clientes tengan conocimiento, en todo momento, del lugar en el que se encuentra su pedido. El mencionado proyecto vulnera el derecho a la privacidad de los trabajadores, por cuanto si bien la medida implantada obedece a un fin constitucionalmente legítimo como es el control del empleado en el desempeño de su puesto de trabajo y la oferta de un mejor servicio al cliente, no supera el necesario juicio de proporcionalidad, dado que el mismo resultado se podría haber obtenido con una menor injerencia en los derechos fundamentales a través de la implantación de sistemas de geolocalización en las motocicletas en las que se transportan los pedidos o a través de pulseras con tales dispositivos, sin que el repartidor tuviera la necesidad de aportar medios propios y, lo que es más importante, datos de carácter personal, como son el número de teléfono o la dirección de correo electrónico en la que han de recibir el código de descarga de la aplicación informática que activa el sistema.

Además, teniendo en cuenta que los datos de localización de una persona, a su vez, son datos de carácter personal, la empresa no informó a los trabajadores del tratamiento que iba a hacer de los mismos, tal y como impone el artículo 5.1 de la Ley Orgánica 15/1999, de Protección de datos de 1999, los actuales 12 y 13 del Reglamento 2016/679 y 11 de la Ley Orgánica 3/2018, de Protección de datos personales y garantía de los derechos digitales. De igual forma, tampoco proporcionó al Comité intercentros información previa apropiada y suficiente que explicara el concreto funcionamiento de la aplicación, esto es, cómo se iba a

[46] STC núm. 186/2000 (rec. 5103/1998).

[47] SAN núm. 13/2019, de 6 de febrero de 2019.

instalar en el teléfono móvil, a qué datos del terminal la misma debería acceder, qué concretos datos propios habría de aportar el trabajador para acceder a la aplicación, qué datos, en su caso, habría de archivar la misma y cómo iban a ser tratados los mismos.

La medida implantada, por consiguiente, se declara nula por vulnerar la legalidad ordinaria, ya que la exigencia de la aportación de un teléfono móvil con conexión de datos para desarrollar el trabajo en los términos efectuados supone un manifiesto abuso de derecho empresarial. Además de quebrar con la necesaria ajenidad en los medios que caracteriza el contrato de trabajo, se responsabiliza al repartidor de cualquier impedimento en la activación del sistema de geolocalización bajo sanción de suspensión del contrato de trabajo con la consiguiente pérdida del salario conforme el artículo 45.2 del ET, lo que implica la adopción de un régimen de infracciones y sanciones, vía contrato individual, obviando el artículo 58.1 del ET que encomienda tal misión a la negociación colectiva.

Empero, en otro supuesto, se rechaza la existencia de una violación del artículo 18 de la CE cuando «en ningún momento el GPS instalado en el coche de la empresa tiene por objeto captar imágenes íntimas de los trabajadores sino facilitar el control, incluso en beneficio de la propia seguridad de los trabajadores (y así se corrobora por las propias intenciones del trabajador recurrente al querer introducir el carácter peligroso de la vigilancia en los polígonos industriales). El uso de medios y dispositivos tipo GPS no se pueden considerar ilícitos, pues la empresa tiene un claro interés en tener localizados sus vehículos, lo que no incide en la violación de ningún derecho fundamental. Finalmente, tampoco parece razonable que la empresa, ante la comisión de faltas laborales, desvele las medidas de control y de seguridad tendentes a prevenir a disuadir o a posibles infractores, cuando se refieren a vigilancia sobre mercancías, que pueden ser sustraídas, o localización de vehículos en sus rutas laborales en un ámbito que no se puede considerar de intimidad o privacidad o de estricto control de una persona con un fin ilegal»[48].

En el mismo sentido, no debe olvidarse que se ha establecido «de forma invariable y constante que las facultades empresariales se encuentran limitadas por los derechos fundamentales (…)[49]. Por ello, al igual que el interés público en sancionar infracciones administrativas resulta insuficiente para que la Administración pueda sustraer al interesado información relativa al fichero y sus datos, según dispone el art. 5.1 y 2 LOPD (…), tampoco el interés privado del empresario podrá justificar que el tratamiento de datos sea empleado en contra del trabajador sin una información previa sobre el control laboral puesto en práctica. No hay en el ámbito laboral, por expresarlo, en otros términos, una razón que tolere la limitación del derecho de información que integra la cobertura

[48] STSJ de Galicia, de 6 de junio de 2014 (rec 903/2014).

[49] Entre otras, SSTC 98/2000, de 10 de abril y 308/2000, de 18 de diciembre.

ordinaria del derecho fundamental del art. 18.4 CE. Por tanto, no será suficiente que el tratamiento de datos resulte en principio lícito, por estar amparado por la Ley (arts. 6.2 LOPD y 20 LET), o que pueda resultar eventualmente, en el caso concreto de que se trate, proporcionado al fin perseguido; el control empresarial por esa vía, antes bien, aunque podrá producirse, deberá asegurar también la debida información previa»[50].

La anterior doctrina indicada infiere, «como cuestión básica y fundamental, a los efectos del posible uso por parte del empresario de mecanismos de vigilancia y control de sus trabajadores que puedan incidir en una posible restricción de un derecho fundamental de estos, y en concreto del contemplado en el art. 18.4 de la CE, la necesaria y suficiente información a dichos trabajadores de su instalación, y de la finalidad que con la misma se persigue. Exigencia, en principio, que, por lo que se refiere al caso examinado se cumplió, siendo ello una cuestión que se declara expresamente acreditada en los hechos probados de la sentencia impugnada, según los cuales el actor tenía conocimiento de que en el vehículo de la empresa que usaba para realiza su trabajo se había instalado un GPS, y, además, el propio actor suscribió un documento sobre tratamiento de datos, en los que prestaba su expresa conformidad (...).

Y sigue diciendo dicha sentencia, como podrá comprobarse, el presente caso requiere de una precisión complementaria, en cuanto que en nuestra primera sentencia ya referenciada valoramos un caso en el que el trabajador conocía la instalación del GPS, y además había suscrito documento en el que daba su conformidad al tratamiento de datos. En el supuesto que nos ocupa sin embargo, se declara expresamente probado que el interesado conocía la instalación del GPS, pero no se considera acreditado que hubiera prestado consentimiento al tratamiento de datos.

Ahora bien, expuesto lo anterior, sigue diciendo dicha sentencia que "como se deriva de la STC 29/2013, de 11 de febrero de 2013, que ya citamos en nuestra anterior resolución, y que se alude de nuevo en el escrito de impugnación del recurso, las obligaciones específicas de información y las autorizaciones necesarias en los casos de tratamiento de datos, se refieren siempre a casos en los que se quiere utilizar la información en cuestión para usos distintos de los inicialmente previstos. En concreto, la mentada STC 29/2013 valora la utilización de la grabación de imágenes en un recinto universitario, cuanto la instalación y la autorización administrativa para ello se referían al control de acceso y seguridad de las dependencias, hasta el punto de que se hace notar que "ni siquiera estaban situados los aparatos de video- vigilancia dentro de las concretas dependencias donde se desarrollaba la prestación laboral, sino en los vestíbulos y zonas de paso públicos". Esto es, no estando previsto ni siendo previsible que las imágenes se usen

[50] STSJ de Castilla-La Mancha, de 23 de marzo de 2015 (rec 1775/2014).

para finalidades distintas de las inicialmente planificadas, entonces la aplicación de un uso diverso requiere de las correspondientes garantías específicas.

Y sigue diciendo dicha sentencia "pero el caso descrito nada tiene que ver con el que ahora nos ocupa, en el que los datos GPS utilizados son única y exclusivamente los generados por el movimiento del vehículo utilizado por el trabajador solo en jornada de trabajo y a los exclusivos efectos de realizar las funciones propias de la categoría. Cuestión distinta es que implantado el sistema GPS en un vehículo puesto a disposición del trabajador de manera permanente, por ejemplo, en caso de directivos o comerciales, resultara luego que se intentaran hacer valer los datos obtenidos en relación a tramos horarios ajenos a la jornada laboral y a la prestación de servicios. Sin embargo si el sistema GPS se instala en el vehículo asignado precisamente para el desarrollo del servicio y para poder realizar las rutas de vigilancia, entonces no acertamos a discernir cómo puede separarse conceptualmente el control de posición de tal vehículo, de la comprobación del cumplimiento de sus obligaciones por parte del trabajador.

Expuesto lo anterior, habrá que concluir con la estimación del recurso, en cuanto la utilización de los datos ha sido para finalidad distintas a las previstas, ya que como queda dicho, el dispositivo de localización por GPS, tenía por finalidad "garantizar la seguridad y coordinación de ellos trabajos", en definitiva, podían utilizarse por la empresa para la comprobación del cumplimiento de los deberes laborales del interesado, pero, como dice la sentencia anteriormente referenciada "cuestión distinta es que implantado el sistema GPS en un vehículo puesto a disposición del trabajador de manera permanente, resultara luego que se intentaran hacer valer los datos obtenidos en relación a tramos horarios ajenos a la jornada laboral y a la prestación de servicios", lo que es el caso, ya que se han utilizado dichos datos, no con la finalidad de control durante su jornada laboral, sino en relación a tramos horarios ajenos a la jornada laboral, como era los periodos de baja por incapacidad temporal, para lo que no se encontraba autorizado, todo lo cual comporta la estimación del presente recurso, con la consiguiente declaración de nulidad del despido acontecido. al quedar constancia de que la actora no era conocedora, de la instalación del GPS, en el vehículo que conducía, para supuesto ajeno al control de su jornada de trabajo»[51].

No solo a nivel nacional hay pronunciamientos al tema de estudio, el Tribunal Europeo de Derechos Humanos ha manifestado que «el sistema GPS instalado en el automóvil que la empresa cedió al demandante por teóricas razones de seguridad se utilizó, en realidad, sin previo aviso, ni información al afectado, para conocer y tratar luego los datos relativos a los lugares en que estuvo en cada momento mientras lo conducía y, de este modo, buscar la probanza del modo en que realizó su prestación laboral, el carácter profesional del uso del vehículo en el exterior de

[51] STSJ de Andalucía, de 19 de octubre de 2017.

la empresa y del trabajo desempeñado no empecen la realidad de una injerencia en los derechos que le asisten a la intimidad personal y protección de datos de esta índole, por lo que el procedimiento utilizado los violentó flagrantemente y, por ello, la prueba así obtenida de que quiere valerse la recurrente carece de eficacia alguna debido a su patente ilicitud»[52].

## 6. CONCLUSIONES

En definitiva, la facultad de control del empresario a través de la geolocalización se tiene que ejercer conforme al marco legal establecido al efecto y con los límites inherentes a aquel. La legitimidad de su uso en el ámbito laboral viene enfocada para que se cumpla con el marco legal aplicable en cada supuesto. Por tanto, los requisitos específicos es que el empleador informe a los trabajadores, por una parte, sobre el uso de un dispositivo GPS y las características de aquel. Por otra, informar, en su caso, a los representantes de los trabajadores. Por último, el derecho que tienen los trabajadores de ejercer los derechos de acceso, rectificación, limitación del tratamiento y supresión de los datos. Se destaca que no se precisa el consentimiento del trabajador, pero se requiere la información antes mencionada.

Dicho de otra manera, las limitaciones que tiene el empleador para utilizar los dispositivos de geolocalización son, por un lado, la de informar de manera «expresa, clara e inequívoca» en cuanto a la existencia y características de aquellos[53]. Por otro, informar a los representantes de los trabajadores. Finalmente, el derecho que tienen los trabajadores, como ya se ha comentado, de ejercer los derechos de acceso, rectificación, limitación del tratamiento y supresión de los datos.

La información se puede facilitar por escrito o a través de medios electrónicos. Por ejemplo, se puede realizar mediante formularios web, formulario en papel, registro en aplicaciones móviles, contratos, cláusulas y enlaces, entre otros. En el caso de que se traten datos personales que no aporte el trabajador, dado que el empresario los tiene, puede enviarse por correo postal con acuse de recibo o por la intranet de la empresa. Lo importante es que el empleador, en su caso, pueda acreditar el cumplimiento de su deber de información con el objeto de verificar el cumplimiento de la obligación[54].

Por tanto, el trabajador debe tener toda la información concerniente, lo ideal es que se utilice el sistema de geolocalización, ya sea vehículo, móvil o cualquier

[52] Sentencia del Tribunal Europeo de Derechos Humanos de 2 de septiembre de 2010.

[53] STSJ de Asturias, de 30 de marzo de 2017 (rec. 2997/2016).

[54] Blazquez Agudo, E., "Nuevas formas de control empresarial: desde los GPS hasta el más allá", en (Dirs. Rodríguez-Piñero Royo, M. y Todolí Signes, A.), *Vigilancia y control en el Derecho del Trabajo Digital*, Thomson Reuters – Aranzadi, Cizur Menor, 2020, págs. 162-163.

otro instrumento de propiedad del empleador, en la jornada de trabajo. Empero, en el supuesto de que se utilizara tanto en la jornada laboral como horarios fuera de aquel (personal) el control solo es justificado en el horario de trabajo.

El segundo apartado del artículo 90 de la LOPD indica de manera expresa que los empleadores tienen que informar sobre la posibilidad de ejercer los derechos de acceso, rectificación, limitación del tratamiento y supresión. Aquellos derechos, evidentemente, tienen que materializarse según lo dispuesto en la norma al efecto; y el responsable del tratamiento, en este caso el empleador, tiene que atender toda solicitud de ejercicio de derechos dentro del plazo de un mes, que puede ampliarse teniendo en consideración la complejidad y el número de solicitudes por dos meses. La redacción de aquel precepto mantiene la interpretación que vienen haciendo con relación al uso de los sistemas de geolocalización en el marco del derecho fundamental a la protección de datos e intimidad[55].

En este sentido, se afirma que tanto el derecho a la intimidad (art. 18.1 de l CE) como la protección de datos de carácter personal (art. 18.4 de la CE) no privan el empleador de implementar herramientas que supongan una intromisión en aquellos, dado que los derechos fundamentales no tienen carácter absoluto; por lo que pueden ser objeto de limitaciones cuando aquellas tiendan de manera exclusiva y proporcionada a la protección de otros derechos y valores – como es la propiedad privada del empleador y la libertad de empresa-[56].

Con relación al principio de proporcionalidad, mecanismo establecido por la doctrina constitucional, se supedita la legitimidad y validez de la medida empresarial adoptada a que sea, por una parte, idónea; es decir, adecuada para conseguir el objetivo propuesto. Por otra, necesaria, en el sentido de que no exista otra medida más moderada que permita alcanzar el objetivo fijado, con iguales resultados. Por último, equilibrada en relación a la finalidad pretendida; dicho en otros términos, proporcionada en sentido estricto de manera que se trate de una

[55] López Balaguer, M. y Ramos Moragues, F., "Derecho a la intimidad y a la protección de datos y licitud de la prueba en el proceso laboral", en AA.VV. (Coords. Monreal Bringsvaerd. E., Thibault Aranda, X. y Jurado Segovia, Á.), *Derecho del Trabajo y Nuevas Tecnologías*, Tirant lo Blanch, Valencia, 2020, pág. 422.

[56] Poquet Catalá, R., "Últimos perfiles del sistema de geolocalización como instrumento del empresario", en AA.VV. (Dirs. Rodríguez-Piñero Royo, M. y Todolí Signes, A.), *Vigilancia y control en el Derecho del Trabajo Digital*, Thomson Reuters – Aranzadi, Cizur Menor, 2020, pág. 191.

medida ponderada, por derivarse de ella más beneficios sobre el interés general que perjuicios sobre otros bienes, especialmente del trabajador en concreto[57].

Por consiguiente, uno de los pilares fundamentales para la licitud del control de los desplazamientos por medio de dispositivos GPS y del tratamiento de los datos personales obtenidos es que la existencia de relación laboral faculta a la empresa para establecer algunos límites a derechos fundamentales de los trabajadores. Cuando finaliza la jornada laboral, las facultades empresariales desaparecen y el contrato deja de constituir un vínculo entre las partes que ampara el poder de la empresa para imponer las medidas implantadas. A partir de ese momento, es imprescindible el consentimiento de los trabajadores para mantener en funcionamiento de aquellos dispositivos y para el análisis automatizado de los datos personales. Es indiferente que, al finalizar la jornada laboral, los trabajadores se hagan cargo de los vehículos que utilizan. La protección por la empresa de sus bienes y el control del uso que de ellos se haga una vez terminada la jornada de trabajo no constituye una excepción a la vigencia de la indicada regla general[58].

Como señala la doctrina, por una parte, hay que esperar «que el escueto régimen jurídico-legal lleve a los órganos judiciales a realizar esta interpretación sistemática en aras a la aplicación del resto de avales reconocidas en la presente Ley de Protección de Datos, tal y como ya se ha venido realizando algún pronunciamiento de suplicación y la propia Agencia de Protección de Datos. En todo caso, de los que no cabe duda es (que) queda excluido el seguimiento intensivo o ilimitado, debiendo existir algún mecanismo que permita desactivar el sistema fuera de las horas de trabajo, pues la geolocalización no debe servir para prolongar la subordinación del trabajador más allá del límite temporal determinado por la prestación pactada y tampoco cabe repercutir los datos obtenido extramuros del tiempo de trabajo en el ámbito contractual»[59].

Por otra, «se ha venido mostrando la importancia que supone un posible fortalecimiento del marco normativo, para que, de esta manera, el trabajador verdaderamente esté informado de que su comportamiento está siendo vigilado de una manera clara y, sobre todo, transparente. Además, en este sentido es igualmente necesario que las partes, dentro de la relación, velen por sus intereses contrapuestos de forma justa, sin que exista una imposición de la libertad de empresa frente a la dignidad de los trabajadores»[60].

[57] *Vid*. Reyes Herreros, J. y Alcaide, L., "Geolocalización de trabajadores", *Actualidad Jurídica Uría Menéndez*, núm. 52, 2019, pág. 73.

[58] STSJ Asturias, de 27 de diciembre de 2017 (rec. 2241/2017).

[59] Rodríguez Escanciano, S., *Derechos laborales digitales: Garantías e interrogantes*, Thomson Reuters – Aranzadi, Cizur Menor, 2019, págs. 231-232.

[60] Araguëz Valenzuela, L., "Relación laboral digitalizada en término de justicia y control tecnológico: especial referencia al sistema de geolocalización", en (Dirs. Rodriguez-Piñero Royo,

Asimismo, avalando la reforma de la legislación laboral se requiere «un nuevo título para regular los derechos fundamentales de los trabajadores en las relaciones laborales, despejando las incertidumbres del ejercicio de dichos derechos fundamentales en igualdad y sin discriminaciones y en relación con las tecnologías de la información y la comunicación, con el entorno tecnológico digital que es una realidad insoslayable, virtualmente ausente del ET»[61].

Por último, se ha valorado que el objeto de estudio se «trata de un planteamiento excesivamente reduccionista, ya que sólo se reconoce a la intimidad y, sin embargo, los trabajadores y empleados públicos también son titulares de los derechos al secreto de las comunicaciones y a la intimidad informática - que a pesar del estrecho parentesco que guardan con el derecho a la intimidad personal, son autónomos e independientes de este -. Además, es simplista por cuanto que los arts. 89 y 90 de la LOPD, en rigor, se limitan a regular el derecho a la intimidad informática de los trabajadores y empleados públicos frente al uso de dispositivos de videovigilancia y de grabación de sonidos y de sistema de geolocalización, remitiéndose en cuanto a las condiciones del ejercicio de las funciones de control a través de estos dispositivos al marco legal correspondiente»[62].

Dicho de otra manera, que al referirse a una normativa que regula perfiles de derechos fundamentales la norma es criticable. Bajo este contexto, «la crítica al legislador puede centrarse, en primer lugar, en la falta de precisión a la hora de configurar la justificación legítima de la empresa para delimitar la intensidad del control. En segundo lugar, en la falta de recepción normativa eficiente de los principios clásicos de la doctrina constitucional de proporcionalidad, idoneidad y necesidad. Y, en tercer lugar, en la debilidad con la que se configura el derecho esencial de información que forma parte de aquellos derechos fundamentales»[63].

M. y Todolí Signes, A.), *Vigilancia y control en el Derecho del Trabajo Digital*, Thomson Reuters – Aranzadi, Cizur Menor, 2020, pág. 216.

[61] Casas Baamonde, M., "Informar antes de vigilar. ¿Tiene el Estado la obligación positiva de garantizar un mínimo de vida privada a los trabajadores en la empresa en la era digital? La necesaria intervención del legislador laboral", *Derecho de las Relaciones Laborales*, núm. 2, 2018, págs. 118-119.

[62] Roqueta Buj, R., "El derecho a la intimidad frente a la videovigilancia en el ámbito laboral", en AA.VV. (Coords. Monreal Bringsvaerd. E., Thibault Aranda, X. y Jurado Segovia, Á.), *Derecho del Trabajo y Nuevas Tecnologías*, Tirant lo Blanch, Valencia, 2020, pág. 253.

[63] López Balaguer, M. y Ramos Moragues, F., "Derecho a la intimidad y a la protección de datos y licitud de la prueba en el proceso laboral", en AA.VV. (Coords. Monreal Bringsvaerd. E., Thibault Aranda, X. y Jurado Segovia, Á.), *Derecho del Trabajo y Nuevas Tecnologías*, Tirant lo Blanch, Valencia, 2020, pág. 423.

Empero, hay que resaltar que aquellos derechos que tienen los trabajadores están sujetos a uno límites, dado que no son absolutos[64]. Por lo que debe tenerse en cuenta que el derecho de supresión no se podrá llevar a cabo cuando el tratamiento de los datos personales obtenidos a través de la geolocalización se requiera necesarios o indispensables en los siguientes supuestos que señala el RGPD:

a) El cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento [art. 17.3 b)].

b) El cumplimiento de una misión realizada en interés público o en ejercicios de poderes públicos conferidos al empleador [art. 17.3 b)].

c) Por razones de interés público en el área de la salud pública [art. 9.2 h) e i) y 3, 17.3 c)].

d) Para la formulación, el ejercicio o la defensa de reclamaciones [art. 17.3 e)].

Por último, hay que destacar que la negociación colectiva, en cualquier caso, es un cause eficaz para que se asuman soluciones equilibradas en un aspecto tan ligado a la intimidad, privacidad y autodeterminación informativa como son los dispositivos de geolocalización. «Aunque no demasiados, los casos de éxito en la negociación colectiva muestran interesantes resultados acerca del fiscalizador del GPS mientras se trabaja y la posibilidad de desconectarlo cuando el vehículo de la empresa está en funciones de uso particular»[65].

Por ello, se afirma que mientras «la norma heterónoma no proceda a alcanzar semejante anhelo, los códigos de conducta, las reglamentaciones internas o los convenios colectivos deben jugar un papel crucial y completar semejante laguna, con el objetivo de dar seguridad jurídica a ambas partes de la relación sobre el uso de geolocalizadores. En este sentido, la empresa debe establecer con carácter previo las reglas sobre utilización de estos dispositivos, qué se puede hacer y qué no está permitido, para inmediatamente después informar a las personas trabajadoras sobre dichas pautas»[66].

[64] Sagardoy De Simón, I., *Nuevas tecnologías y relaciones laborales*, Francis Lefebvre, Madrid, 2020, págs. 53 y 54.

[65] Cuadros Garrido, M., "La protección de los derechos fundamentales de la persona trabajadora ante la utilización de GPS: ¿reformulación o continuidad?", *Lan Harremanak: Revista de Relaciones Laborales*, núm. 42, 2020, pág. 17.

[66] Fernández Fernández, R., "La geolocalización como mecanismo de control laboral: alcance y límites de una controvertida herramienta del poder directivo", *Revista de Trabajo y Seguridad Social. CEF*, núm. 452, 2020, págs. 145-46.